

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-256136

(43)Date of publication of application : 21.09.2001

(51)Int.Cl.

G06F 13/00

H04L 12/46

H04L 12/28

H04L 12/66

(21)Application number : 2000-065145

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 09.03.2000

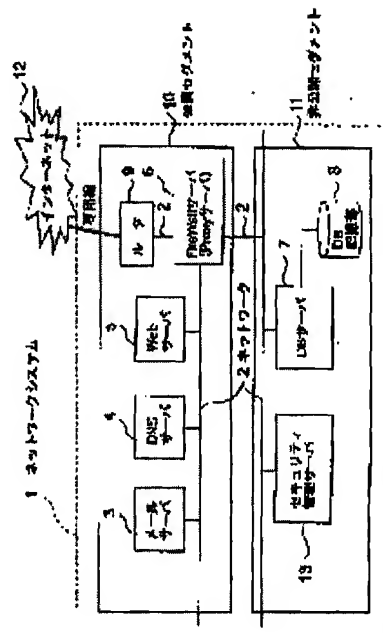
(72)Inventor : NEZU KIMISUKE

(54) NETWORK SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To unitarily manage the security information of respective computers and to automate the setting work of the security information performed by a manager by manual work.

SOLUTION: This network system 1 constituted of the plural computers 3-9 is provided with a security information setting means 13 for storing the security information composed of at least one of user information for defining a user permitted to use the present computer, access information for defining the computer which the present computer is permitted to access and to-be-accessed information for defining the computer permitted to access the present computer and set for the respective computers 3-9 and setting the security information to the respective computers 3-9 based on the stored security information.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-256136

(P2001-256136A)

(43) 公開日 平成13年9月21日 (2001.9.21)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 8 9
H 0 4 L 12/46		H 0 4 L 11/00	3 1 0 C 5 K 0 3 0
12/28		11/20	B 5 K 0 3 3
12/66			9 A 0 0 1

審査請求 未請求 請求項の数4 O L (全 7 頁)

(21) 出願番号 特願2000-65145 (P2000-65145)

(22) 出願日 平成12年3月9日 (2000.3.9)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 根津 公輔

東京都府中市東芝町1番地 株式会社東芝

府中工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B089 GA11 KA17 KB13

5K030 GA15 GA17 HA08 HC14 HD03

HD06 JA00 JT06 LD20

5K033 AA08 BA04 CC01 DA01 DA06

9A001 BB02 BB03 BB04 CC02 DD10

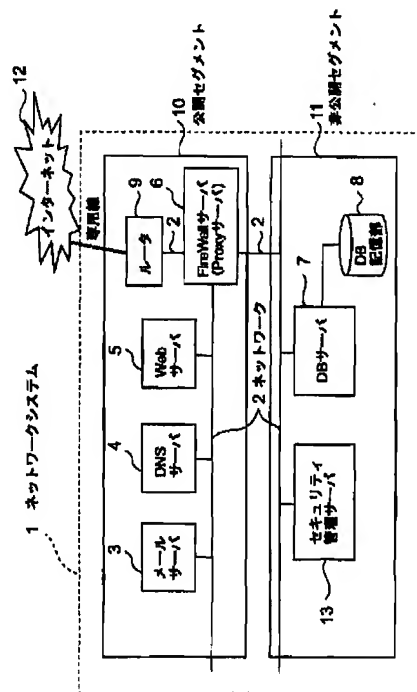
JJ18 JJ27 JJ25 KK56 LL03

(54) 【発明の名称】 ネットワークシステム

(57) 【要約】

【課題】 各計算機のセキュリティ情報を一元的に管理するとともに、管理者がマニュアル作業で行っていたセキュリティ情報の設定作業を自動化すること。

【解決手段】 複数の計算機3～9から構成されてなるネットワークシステム1において、自己計算機の使用を許可されたユーザを定義したユーザ情報、自己計算機がアクセス許可された計算機を定義したアクセス情報、自己計算機にアクセス許可された計算機を定義した被アクセス情報のうちの少なくとも1つからなり、各計算機3～9毎に設定されたセキュリティ情報を記憶するとともに、記憶したセキュリティ情報に基づいて各計算機3～9に対してセキュリティ情報を設定するセキュリティ情報設定手段13を備える。



【特許請求の範囲】

【請求項1】 複数の計算機から構成されてなるネットワークシステムにおいて、

自己計算機の使用を許可されたユーザを定義したユーザ情報、自己計算機がアクセス許可された計算機を定義したアクセス情報、自己計算機にアクセス許可された計算機を定義した被アクセス情報のうちの少なくとも1つからなり、前記各計算機毎に設定されたセキュリティ情報を記憶するとともに、記憶したセキュリティ情報に基づいて前記計算機に対してセキュリティ情報を設定するセキュリティ情報設定手段を備えたことを特徴とするネットワークシステム。

【請求項2】 請求項1に記載のネットワークシステムにおいて、

前記セキュリティ情報に変更があった場合には、その変更内容に基づいて、記憶しているセキュリティ情報を更新し、前記更新されたセキュリティ情報に基づいて前記計算機に対してセキュリティ情報を設定するセキュリティ情報変更手段を備えたことを特徴とするネットワークシステム。

【請求項3】 請求項1または請求項2に記載のネットワークシステムにおいて、

前記計算機のセキュリティ情報が設定された場合には、前記各計算機に設定されたセキュリティ情報の整合性を確認するセキュリティ情報確認手段を備えたことを特徴とするネットワークシステム。

【請求項4】 請求項1乃至3のうちいずれか1項に記載のネットワークシステムにおいて、

前記各計算機は、当該ネットワークシステム自体を他のネットワークシステムに接続するルータ、前記他のネットワークシステムから当該ネットワークシステム自体へのアクセス要求を前記ルータを介して取得し、前記セキュリティ情報で許可された内容の前記アクセス要求のみを要求先の計算機に配信するファイヤウォール、ホームページ情報を格納しており、前記ホームページ情報の閲覧要求を受けた場合には、前記ホームページ情報を要求元に返信するWebサーバのうちの少なくともいずれかとしたことを特徴とするネットワークシステム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、複数の計算機から構成されてなるネットワークシステムに係り、更に詳しくは、各計算機のセキュリティ情報を一元的に管理するとともに、その管理内容に基づいて、各計算機のセキュリティ情報を設定するネットワークシステムに関するものである。

【0002】

【従来の技術】 最近、複数の計算機を、ネットワークを介して互いに接続することにより、機能の分散、およびシステムの拡張等に対する柔軟性を高めたネットワーク

システムが広く用いられている。

【0003】 この種のネットワークシステムは、各計算機毎に、自己計算機の使用を許可されたユーザを定義したユーザ認証情報、自己計算機がアクセス可能な計算機を定義したり、逆に自己計算機にアクセス可能な計算機を定義したアクセス情報等からなるセキュリティ情報を設定している。これによって、ネットワークシステムを使用するユーザを特定することができるとともに、セキュリティレベルに応じて各計算機を機能的に分散することにより管理し、システム全体の保全性を高めている。

【0004】 図4は、この種の従来から用いられているネットワークシステムの一例を示す構成図である。

【0005】 この種のネットワークシステム20は、ネットワーク2を介して互いに接続されたメールサーバ3、DNS（ドメインネームシステム）サーバ4、Webサーバ5、ファイヤウォールサーバ（プロキシサーバ）6、データベースサーバ7、データベース記憶部8等から構成される。更に、このネットワークシステム20をインターネット12等の他のネットワークシステムに接続する場合には、ルータ9が備えられている。

【0006】 メールサーバ3には、ネットワーク20内から発信する、あるいはネットワーク20内へ送信されたメールデータが一旦格納される。そして、これらメールデータは、メールサーバ3に一旦格納された後に、メールサーバ3から、宛先として指定されたユーザ宛に送信される。

【0007】 DNSサーバ4では、Webサーバ5に格納されているホームページ情報に対応したドメイン名が管理される。

【0008】 Webサーバ5には、ホームページ情報が格納される。

【0009】 ファイヤウォールサーバ（プロキシサーバ）6では、インターネット12を介してネットワークシステム20の外からアクセスしてきたユーザに対して、そのセキュリティレベルがチェックされ、そのセキュリティレベルに応じて、アクセス要求するサーバへのアクセスが管理される。

【0010】 データベースサーバ7では、データベース記憶部8に記憶されているデータベースが管理され、追加データのデータベース記憶部8への記憶や、データベース記憶部8に記憶されているデータの参照や、更新等の入力操作がなされる。

【0011】 データベース記憶部8では、種々のデータベースが記憶される。

【0012】 また、インターネット12を介してネットワークシステム20側にアクセスしてきたアクセス要求は、そのアクセス要求先情報と関連付けられてルータ9に取り込まれ、更にそこからファイヤウォールサーバ6に送信される。

【0013】 図4に示すネットワークシステム20にお

10

20

30

40

50

いて、メールサーバ3、DNSサーバ4、Webサーバ5、ファイヤウォールサーバ6、ルータ9は公開セグメント10と呼ばれ、ネットワークシステム20のユーザのみならず、インターネット12を介してこのネットワークシステム20の外からアクセスしてきたユーザに対してもアクセスが許可されている。

【0014】一方、図4に示すネットワークシステム20において、データベースサーバ7およびデータベース記憶部8は非公開セグメント11と呼ばれ、この非公開セグメント11へのアクセスは、ネットワークシステム20のユーザのみに限られ、インターネット12を介してこのネットワークシステム20の外からアクセスしてきたユーザに対してはアクセスが許可されていない。

【0015】このようなアクセス許可/非許可の設定は、各計算機毎にセキュリティ情報を設定することによってなされる。

【0016】セキュリティ情報には、図5に示すように、自己計算機の使用を許可されたユーザを定義したユーザ認証情報、自己計算機がアクセス可能な計算機を定義したり、逆に自己計算機にアクセス可能な計算機を定義したアクセス制限情報、発信または受信するデータの暗号化に関する設定を行う暗号化情報が含まれている。

【0017】そして、図6にその一例を示すように、ネットワークシステム20を構成している各計算機は、おのおのセキュリティ情報が個別に設定されている。

【0018】メールサーバ3は、ユーザ認証情報として管理者のみが設定されており、指定された管理者のみがこのメールサーバ3を直接使用することができる。また、アクセス制限情報として全ユーザに対してread/write可とされており、全ユーザに対してアクセスが許可され、アクセス許可された領域のメールデータを参照したり、書き込んだりすることが許可されている。

【0019】DNSサーバ4は、ユーザ認証情報として管理者のみが設定されており、指定された管理者のみがDNSサーバ4を直接使用することができる。また、アクセス制限情報としてネットワークシステム20のユーザに対してread/write可、それ以外のユーザに対してread可とされており、ネットワークシステム20のユーザに対してはアクセスが許可され、アクセス許可された領域のDNSデータを参照したり、書き込んだりすることが許可されている。また、ネットワークシステム20外のユーザに対しては、アクセス許可された領域のDNSデータを参照することのみ許可されている。

【0020】Webサーバ5も、ユーザ認証情報とアクセス制限情報に関しては、DNSサーバ4と同内容のセキュリティ情報が設定されている。また、Webサーバ5では、更に、暗号化情報について、暗号化すると設定されており、これによって、Webサーバ5からインターネット12側に出力されるデータ情報は暗号化された後に出力される。

【0021】ファイヤウォールサーバ6は、ユーザ認証情報として管理者のみが設定されており、指定された管理者のみがファイヤウォールサーバ6を直接使用することができる。また、アクセス制限情報(対他マシン)として公開セグメント10側にのみアクセス可とされており、これによって、インターネット12を介してネットワークシステム20外からファイヤウォールサーバ6にアクセスしてきた情報は、公開セグメント10にある計算機のみアクセスされる。一方、アクセス制限情報(対自マシン)としては、管理者のみread/write可、それ以外のユーザはread可と設定されており、これによって、アクセス許可された領域のデータを参照することは全ユーザに対して許可されているが、データの書き込みは管理者のみに許可されている。

【0022】データベースサーバ7は、ユーザ認証情報として管理者のみが設定されており、指定された管理者のみがデータベースサーバ7を直接使用することができる。また、アクセス制限情報としてネットワークシステム20のユーザに対してread/write可とされており、ネットワークシステム20のユーザに対してはアクセスが許可され、アクセス許可された領域のDNSデータを参照したり、書き込んだりすることが許可されている。

【0023】ルータ9は、アクセス制限情報としてネットワークシステム20のユーザに対してread/write可、それ以外のユーザに対してread可とされており、ネットワークシステム20のユーザに対してはアクセスが許可され、アクセス許可された領域のルータデータを参照したり、書き込んだりすることが許可されている。また、ネットワークシステム20外のユーザに対しては、アクセス許可された領域のルータデータを参照することのみ許可されている。

【0024】ネットワークシステム20を構成している各計算機は、このように、おのおのの計算機毎に設定されたセキュリティ情報の内容に基づいて、使用ユーザ、アクセス制限、および暗号化等の管理がなされている。

【0025】

【発明が解決しようとする課題】しかしながら、このような従来のネットワークシステムでは、以下のような問題がある。

【0026】すなわち、このような各計算機のセキュリティ情報の設定は、ネットワークシステム20の管理者が、各計算機について定めたセキュリティ情報の内容を参照しながら、各計算機毎にマニュアルで設定していた。

【0027】このため、ネットワークシステム20を構成している計算機の数が多くなり、そのシステム構成が複雑になるほど、管理者の負担が増加するばかりでなく、設定ミスが生じる可能性も高くなるという問題がある。

【0028】また、システムを変更した場合には、その

変更内容に基づいて、該当する計算機のセキュリティ情報をマニュアルで変更する必要があるために、この場合にも、上述同様の問題が発生する。

【0029】本発明はこのような事情に鑑みてなされたものであり、ネットワークを構成している各計算機毎に設定されたセキュリティ情報を記憶するとともに、その記憶内容に基づいて、各計算機に対してセキュリティ情報を設定し、もって、各計算機のセキュリティ情報を一元的に管理するとともに、管理者がマニュアル作業で行っていたセキュリティ情報の設定作業を自動化することができるネットワークシステムを提供することを目的とする。

【0030】

【課題を解決するための手段】上記の目的を達成するために、本発明では、以下のような手段を講じる。

【0031】すなわち、請求項1の発明では、複数の計算機から構成されてなるネットワークシステムにおいて、自己計算機の使用を許可されたユーザを定義したユーザ情報、自己計算機がアクセス許可された計算機を定義したアクセス情報、自己計算機にアクセス許可された計算機を定義した被アクセス情報のうちの少なくとも1つからなり、各計算機毎に設定されたセキュリティ情報を記憶するとともに、記憶したセキュリティ情報に基づいて計算機に対してセキュリティ情報を設定するセキュリティ情報設定手段を備える。

【0032】従って、請求項1の発明のネットワークシステムにおいては、以上のような手段を講じることにより、定義されたセキュリティ情報に基づいて、各計算機のセキュリティ情報を設定することができる。

【0033】請求項2の発明では、請求項1の発明のネットワークシステムにおいて、セキュリティ情報に変更があった場合には、その変更内容に基づいて、記憶しているセキュリティ情報を更新し、更新されたセキュリティ情報に基づいて計算機に対してセキュリティ情報を設定するセキュリティ情報変更手段を備える。

【0034】従って、請求項2の発明のネットワークシステムにおいては、以上のような手段を講じることにより、変更されたセキュリティ情報に基づいて、各計算機のセキュリティ情報を変更することができる。

【0035】請求項3の発明では、請求項1または請求項2の発明のネットワークシステムにおいて、計算機のセキュリティ情報が設定された場合には、各計算機に設定されたセキュリティ情報の整合性を確認するセキュリティ情報確認手段を備える。

【0036】従って、請求項3の発明のネットワークシステムにおいては、以上のような手段を講じることにより、各計算機に設定されたセキュリティ情報の整合性を確認することができる。

【0037】請求項4の発明では、請求項1乃至3のうちいずれか1項の発明のネットワークシステムにおい

て、各計算機は、当該ネットワークシステム自体を他のネットワークシステムに接続するルータ、他のネットワークシステムから当該ネットワークシステム自体へのアクセス要求をルータを介して取得し、セキュリティ情報で許可された内容のアクセス要求のみを要求先の計算機に配信するファイヤウォール、ホームページ情報を格納しており、ホームページ情報の閲覧要求を受けた場合には、ホームページ情報を要求元に返信するWebサーバのうちの少なくともいずれかとする。

10 【0038】従って、請求項4の発明のネットワークシステムにおいては、以上のような手段を講じることにより、ルータ、ファイヤウォール、Webサーバといった計算機を対象に、セキュリティ情報の設定または変更をしたり、設定または変更されたセキュリティ情報の整合性を確認することができる。

【0039】

【発明の実施の形態】以下に、本発明の実施の形態について図面を参照しながら説明する。

20 【0040】なお、以下の各実施の形態の説明に用いる図中の符号は、図4と同一部分については同一符号を付して示すことにする。

【0041】本発明の実施の形態を図1から図3を用いて説明する。

【0042】図1は、本発明の実施の形態に係るネットワークシステムの一例を示す構成図である。

【0043】本発明の実施の形態に係るネットワークシステム1は、図4に示す従来技術によるネットワークシステム20において、非公開セグメント11側のネットワーク2に接続されたセキュリティ管理サーバ13を付加した構成としている。

30 【0044】このセキュリティ管理サーバ13は、ネットワークシステム1における各計算機3～9のセキュリティ情報を記憶するとともに、記憶したセキュリティ情報の内容に基づいて、各計算機のセキュリティ情報を設定する。

【0045】更に、設定されたセキュリティ情報が、各計算機3～9間で整合しているかを確認し、整合性が取られていない場合には、それを管理者側に報知してセキュリティ情報の再設定を促す。

40 【0046】次に、以上のように構成した本発明の実施の形態に係るネットワークシステム1の作用について説明する。

【0047】まず、ネットワークシステム1における各計算機3～9にセキュリティ情報を新規に設定する場合における作用について図2のフローチャートを用いて説明する。

50 【0048】ネットワークシステム1における各計算機にセキュリティ情報を新規に設定する場合には、管理者による入力操作によって、図6に示すような各計算機毎に定義されたセキュリティ情報の内容に対する情報が、

セキュリティ管理サーバ13に入力され(S1)記憶される(S2)。これは、たとえば、ユーザ認証情報については、ユーザ名が一覧されたテーブルにおいて、認証されたユーザ名をチェックすることによって、アクセス制限情報については、ユーザ名が一覧されたテーブルにおいて、権限内容(アクセス不可、readのみ、writeのみ、read/write両方)欄の該当箇所をチェックすることによって行われる。

【0049】セキュリティ管理サーバ13にセキュリティ情報が記憶されると、ネットワークシステム1に接続している各計算機3~9は、セキュリティ管理サーバ13によって、セキュリティ管理サーバ13が記憶している内容に従って、セキュリティ情報が設定される(S3)。

【0050】更に、設定されたセキュリティ情報が各計算機3~9の間で整合性が取られているかが確認され(S4)、各計算機3~9間で設定されたセキュリティ情報の不整合がない場合(S5:Yes)には、セキュリティ情報の設定が完了し、不整合がある場合(S5:No)には、ステップS1に戻る。

【0051】次に、ネットワークシステム1における各計算機3~9のうちのいずれかのセキュリティ情報を変更する場合、あるいはネットワークシステム1に新たな計算機を追加し、その計算機についてセキュリティ情報を設定する場合における作用について図3のフローチャートを用いて説明する。

【0052】ネットワークシステム1における各計算機3~9のうちのいずれかのセキュリティ情報を変更する場合、あるいはネットワークシステム1に新たな計算機を追加する場合には、管理者による入力操作によって、既にセキュリティ管理サーバ13に記憶されているセキュリティ情報の内容が変更されるか、あるいは追加される計算機のセキュリティ情報が追加されることによって記憶内容が更新される(S11)。

【0053】セキュリティ管理サーバ13のセキュリティ情報が更新されると、該当する計算機は、セキュリティ管理サーバ13によって、更新内容に従って、セキュリティ情報が設定される(S12)。

【0054】更に、設定されたセキュリティ情報が各計算機3~9の間で整合性が取られているかが確認され(S13)、各計算機3~9間でセキュリティ情報の不整合がない場合(S14:Yes)には、セキュリティ情報の変更設定が完了し、不整合がある場合(S14:No)には、ステップS11に戻る。

【0055】なお、請求項でいうセキュリティ情報設定手段、セキュリティ情報変更手段、セキュリティ情報確認手段は、本発明の実施の形態においてセキュリティ管理サーバ13に該当する。

【0056】上述したように、本発明の実施の形態に係るネットワークシステム1においては、上記のような作

用により、各計算機3~9のセキュリティ情報を一元的に管理するとともに、その管理内容に基づいて各計算機3~9に対してセキュリティ情報を設定したり、変更したりすることができる。

【0057】更に、各計算機3~9について設定または変更されたセキュリティ情報について不整合が無いことを確認することができる。

【0058】以上により、各計算機のセキュリティ情報を一元的に管理するとともに、管理者がマニュアル作業で行っていたセキュリティ情報の設定作業を自動化することが可能となる。

【0059】これによって、管理者の負担を軽減するとともに、セキュリティ情報の変更や、計算機の追加等に適したネットワークシステムを実現することが可能となる。

【0060】以上、本発明の好適な実施の形態について、添付図面を参照しながら説明したが、本発明はかかる構成に限定されない。特許請求の範囲に記載された技術的思想の範疇において、当業者であれば、各種の変更例及び修正例に想到し得るものであり、それら変更例及び修正例についても本発明の技術的範囲に属するものと了解される。

【0061】

【発明の効果】以上説明したように、本発明のネットワークシステムによれば、ネットワークを構成している各計算機毎に設定されたセキュリティ情報を記憶するとともに、その記憶内容に基づいて、各計算機に対してセキュリティ情報を設定することができる。

【0062】以上により、各計算機のセキュリティ情報を一元的に管理するとともに、管理者がマニュアル作業で行っていたセキュリティ情報の設定作業を自動化することが可能となる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係るネットワークシステムの一例を示す構成図。

【図2】計算機にセキュリティ情報を設定する場合の作用を示すフローチャート。

【図3】計算機に、変更されたセキュリティ情報を設定する場合の作用を示すフローチャート。

【図4】従来から用いられているネットワークシステムの一例を示す構成図。

【図5】セキュリティ情報の種類とその内容の一例を示す図。

【図6】各計算機毎に設定されたセキュリティ情報の一例を示す図。

【符号の説明】

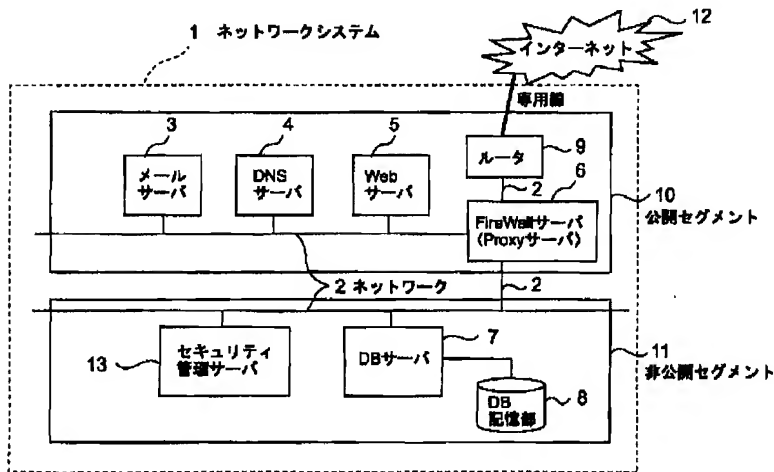
- 1、20・・・ネットワークシステム、
- 2・・・ネットワーク、
- 3・・・メールサーバ、
- 4・・・DNSサーバ、

5・・・Webサーバ、
 6・・・ファイヤウォール、
 7・・・データベースサーバ、
 8・・・データベース記憶部、
 9・・・ルータ、

* 10・・・公開セグメント、
 11・・・非公開セグメント、
 12・・・インターネット、
 13・・・セキュリティ管理サーバ。

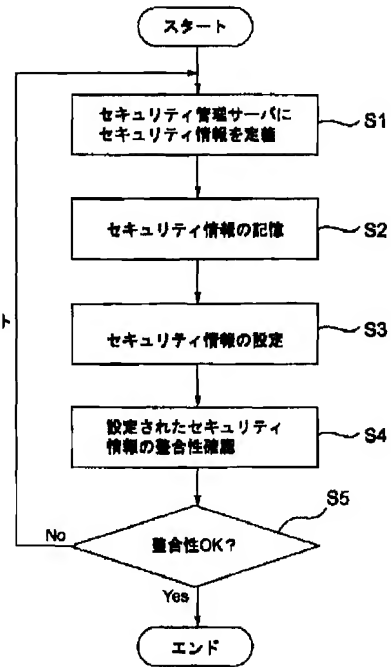
*

【図1】



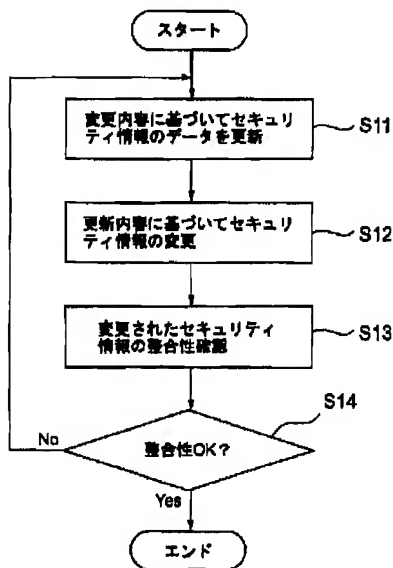
【図2】

<セキュリティ情報の初期設定時>

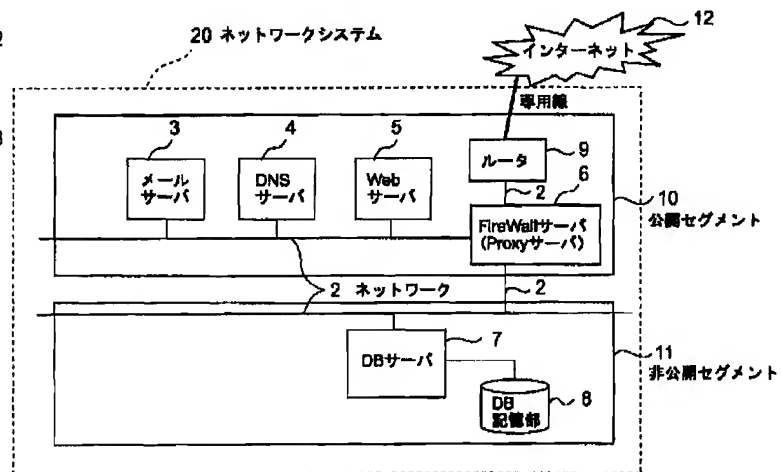


【図3】

<セキュリティ情報の変更時>



【図4】



【図5】

セキュリティ情報	詳細
ユーザ認証情報	ユーザに対する定義
アクセス制限情報	リソースに対する設定
暗号化情報	暗号化の設定

【図6】

マシン	セキュリティ情報	設定内容
メールサーバ 3	ユーザ認証情報	管理者のみ
	アクセス制限情報	全ユーザread/write可
DNSサーバ 4	ユーザ認証情報	管理者のみ
	アクセス制限情報	ネットワークシステムのユーザread/write可、それ以外のユーザread可
Webサーバ 5	ユーザ認証情報	管理者のみ
	アクセス制限情報	ネットワークシステムのユーザread/write可、それ以外のユーザread可
	暗号化情報	する
FireWallサーバ 6	ユーザ認証情報	管理者のみ
	アクセス制限情報 (対他マシン)	公開セグメント側のみアクセス可
	アクセス制限情報 (対自マシン)	管理者のみread/write可、それ以外のユーザread可
DBサーバ 7	ユーザ認証情報	管理者のみ
	アクセス制限情報	ネットワークシステムのユーザread/write可
ルータ 9	アクセス制限情報	ネットワークシステムのユーザread/write可、それ以外のユーザread可